(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 592 853**

(51) Int. CI.:

E05B 47/00 (2006.01)
G07C 9/00 (2006.01)
E05B 47/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **25.06.2010 PCT/EP2010/059041**

(87) Fecha y número de publicación internacional: **13.01.2011 WO11003749**

(96) Fecha de presentación y número de la solicitud europea: **25.06.2010 E 10726106 (7)**

(97) Fecha y número de publicación de la concesión europea: **22.06.2016 EP 2452316**

(54) Título: **Procedimiento de funcionamiento de un sistema de control de acceso**

(30) Prioridad:

06.07.2009 EP 09164689

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.12.2016

(73) Titular/es:

INVENTIO AG (100.0%)
Seestrasse 55
6052 Hergiswil , CH

(72) Inventor/es:

FRIEDLI, PAUL y
SCHWARZENTRUBER, JOSEF

(74) Agente/Representante:

AZNÁREZ URBIETA, Pablo

DESCRIPCIÓN

Procedimiento de funcionamiento de un sistema de control de acceso

La invención se refiere a un procedimiento para el funcionamiento de un sistema de control de acceso y a un sistema de control de acceso según el preámbulo de las reivindicaciones independientes 1 y 8.

El documento WO2008/089207A1 describe un procedimiento de funcionamiento de un sistema de control de acceso para controlar el acceso a una zona protegida de un edificio, como una planta o una sección de una planta. El sistema de control de acceso comprende una unidad informática central y un abrepuertas. El abrepuertas da acceso a una zona protegida. La unidad informática central está en comunicación con el abrepuertas mediante unos puntos de acceso asistidos por red. El abrepuertas incluye un lector que lee un código de identificación de un soporte de datos portátil. El código de identificación leído les comprobado por el lector o bien por la unidad informática central con un código de identificación de una lista con códigos de identificación válidos para la zona protegida. Si la comprobación tiene éxito, el abrepuertas da acceso a la zona protegida.

La WO 2006/056085 A1 describe también un sistema de control de acceso gestionado centralmente. El objetivo de la presente invención es perfeccionar este procedimiento o sistema.

Este objetivo se logra mediante las características identificativas de las reivindicaciones independientes 1 y 8.

En el procedimiento según la invención de funcionamiento de un sistema de control de acceso, el sistema de control de acceso incluye al menos un herraje de puerta a una zona protegida de un edificio y al menos un código de identificación en un soporte de datos portátil; código de identificación que es leído por un lector de un herraje de puerta; dándose acceso a la zona protegida por el herraje de puerta si el código de identificación leído es válido; transmitiendo una unidad informática un código de autorización a una unidad informática central mediante como mínimo un enlace de comunicación; comprobándose si el código de autorización coincide con un código de autorización válido para un perfil de zona; permitiéndose derechos de lectura y escritura para el perfil de zona a la unidad informática que transmite el código de autorización si la comprobación del código de autorización transmitido tiene éxito; modificando la unidad informática el perfil de zona permitido mediante un enlace de comunicación.

Esto tiene la ventaja de que desde una unidad informática cualquiera puede modificarse un perfil de zona con un código de identificación válido para una zona protegida del edificio, lo que hace que el funcionamiento del sistema de control de acceso sea sencillo y flexible. La unidad informática debe comprobar con un código de autorización que está autorizada para esta modificación del perfil de zona en una unidad informática central. La validez de este código de autorización se comprueba. La transmisión del código de autorización y la modificación del perfil de zona permitido se realizan mediante un enlace de comunicación. De este modo, el funcionamiento del sistema de control de acceso es seguro.

En las reivindicaciones dependientes se describen perfeccionamientos ventajosos del procedimiento.

Resulta ventajoso que la unidad informática registre en el perfil de zona permitido, como código de identificación válido, un código de identificación de un soporte de datos portátil. Resulta ventajoso que la unidad informática elimine del perfil de zona permitido un código de identificación de un soporte de datos portátil como código de identificación válido.

Esto tiene la ventaja de que desde la unidad informática puede registrarse en y/o eliminarse del perfil de zona un código de identificación válido de un soporte de datos portátil. Ni la unidad informática ni el soporte de datos portátil deben hallarse físicamente en el sitio del herraje de puerta y/o de la unidad informática central, lo que hace que el funcionamiento del sistema de control de acceso sea sencillo y flexible.

Resulta ventajoso que la unidad informática modifique la validez del código de identificación del perfil de zona permitido. Resulta ventajoso que la unidad informática registre una entidad en el perfil de zona permitido. Resulta ventajoso que la unidad informática elimine una entidad del perfil de zona permitido. Resulta ventajoso que la unidad informática modifique un derecho de lectura de una entidad del perfil de zona permitido. Resulta ventajoso que la unidad informática modifique un derecho de escritura de una entidad del perfil de zona permitido. Resulta ventajoso que la unidad informática modifique una zona horaria de una entidad del perfil de zona permitido.

Esto tiene la ventaja de que desde la unidad informática puede realizarse el mantenimiento de múltiples datos del perfil de zona permitido, lo que hace que el funcionamiento del sistema de control de acceso sea sencillo y flexible.

Además, la unidad informática crea un código de identificación de un soporte de datos portátil en un perfil de zona permitido como código de identificación provisional; y, si el lector del herraje de puerta que da acceso a la zona protegida del perfil de zona permitido lee un código de identificación que coincide con el código de identificación provisional, el código de identificación leído se registra en el perfil de zona permitido como código de identificación válido.

Esto tiene la ventaja de que la unidad informática crea primero un código de identificación provisional de un soporte de datos portátil en el perfil de zona permitido y el código de identificación leído no se registra en el perfil de zona permitido como código de identificación válido hasta haberse realizado realmente la lectura del código de identificación provisional. Así, no se registra en el perfil de zona un código de identificación nuevo hasta que éste ha sido leído realmente por el lector, lo que hace que el funcionamiento del sistema de control de acceso sea seguro. Esto hace también que no sea necesario un lector en la unidad informática para registrar un código de identificación en un perfil de zona, lo que hace que el sistema de control de acceso sea sencillo y económico.

Resulta ventajoso que se cree un código de identificación provisional indicando una serie de cifras en un perfil de zona permitido; y que, si el lector del herraje de puerta que da acceso a la zona protegida del perfil de zona permitido lee una serie de cifras que coincide con la serie de cifras del código de identificación provisional, se registre en el perfil de zona permitido como código de identificación válido un código de identificación leído con la serie de cifras.

Esto tiene la ventaja de que la unidad informática no debe registrar un código de identificación completo en el perfil de zona permitido, sino que basta con que se registren partes del código de identificación, por ejemplo las primeras dos o tres cifras del código de identificación, en el perfil de zona permitido. También puede bastar con registrar datos del perfil de zona, por ejemplo un apellido o un nombre de pila, en el perfil de zona permitido y, al leerse estos datos, registrar en el perfil de zona como código de identificación válido el código de identificación leído con estos datos. Esto hace que el funcionamiento del sistema de control de acceso sea sencillo y flexible.

Resulta ventajoso que se cree un código de identificación provisional indicando un intervalo de tiempo en un perfil de zona permitido; y que, si el lector del herraje de puerta que da acceso a la zona protegida del perfil de zona permitido lee durante este intervalo de tiempo un código de identificación que coincide con el código de identificación provisional, se registre como código de identificación válido en el perfil de zona permitido el código de identificación leído.

Esto tiene la ventaja de que la unidad informática no debe registrar ningún código de identificación en el perfil de zona permitido, sino que, por ejemplo, se registra como código de identificación válido en el perfil de zona el código de identificación leído siguiente en cuanto al tiempo, lo que hace que el funcionamiento del sistema de control de acceso sea sencillo y flexible.

Resulta ventajoso que la unidad informática central transmita a un herraje de puerta, mediante un enlace de comunicación, como mínimo una parte de un perfil de zona para la zona protegida por el herraje de puerta; y que un procesador de un herraje de puerta compruebe si el código de identificación leído por el lector del herraje de puerta coincide con un código de identificación válido del perfil de zona transmitido para la zona protegida por el herraje de puerta. Resulta ventajoso que el perfil de zona se almacene, como mínimo parcialmente, en una memoria de datos legible por ordenador de la unidad informática central. Resulta ventajoso que el perfil de zona se almacene, como mínimo parcialmente, en una memoria de datos legible por ordenador del herraje de puerta. Resulta ventajoso que la unidad informática central transmita mediante un enlace de comunicación a un herraje de puerta como mínimo una parte de un perfil de zona para la zona protegida por el herraje de puerta; que un procesador de un herraje de puerta compruebe si un código de identificación leído por el lector del herraje de puerta coincide con un código de identificación válido del perfil de zona transmitido para la zona protegida por el herraje de puerta; que, si la comprobación del código de identificación leído tiene éxito, el procesador transmita una señal de acceso a un actuador del herraje de puerta; y que el actuador dé acceso a la zona protegida por el herraje de puerta para la señal de acceso transmitida. Esto tiene la ventaja de que un procesador de un herraje de puerta comprueba *in situ* si un código de identificación leído por el lector del herraje de puerta coincide con un código de identificación válido del perfil de zona para la zona protegida por el herraje de puerta, lo que hace que el funcionamiento del sistema de control de acceso sea rápido, ya que el herraje de puerta no necesita realizar consultas, que gastarían tiempo, a la unidad informática central, que está alejada del herraje de puerta, con fines de comprobación. La comunicación del perfil de zona para la zona protegida por el herraje de puerta al lector

puede realizarse a intervalos de tiempo regulares y/o irregulares, por ejemplo en caso de ser necesaria una actualización del perfil de zona almacenado en la memoria de datos legible por ordenador del herraje de puerta. Tampoco es necesario transmitir todo el perfil de zona, sino que basta con transmitir una parte del perfil de zona, lo que reduce el tiempo de transmisión. Por ejemplo, se transmite sólo una parte modificada del perfil de zona.

Resulta ventajoso que un código de identificación leído por un lector se transmita mediante un enlace de comunicación a la unidad informática central. Resulta ventajoso que la unidad informática central compruebe si un código de identificación leído por un lector de un herraje de puerta coincide con un código de identificación válido de un perfil de zona para la zona protegida por el herraje de puerta del lector. Resulta ventajoso que, si la comprobación del código de identificación leído tiene éxito, la unidad informática central transmita una señal de acceso a un actuador del herraje de puerta mediante el enlace de comunicación; y que el actuador dé acceso a la zona protegida por el herraje de puerta para la señal de acceso transmitida.

Esto tiene la ventaja de que la unidad informática central remota comprueba si un código de identificación leído por el lector coincide con un código de identificación válido del perfil de zona para la zona protegida por el herraje de puerta del lector, lo que hace que el funcionamiento del sistema de control de acceso sea seguro.

Resulta ventajoso que la unidad informática central transmita a una unidad informática de edificio, mediante un enlace de comunicación, un código de autorización transmitido; que la unidad informática de edificio compruebe si el código de autorización transmitido coincide con un código de autorización válido para un perfil de zona; y que, si la comprobación del código de autorización transmitido tiene éxito, la unidad informática de edificio transmita mediante un enlace de comunicación a la unidad informática central una señal de autorización. Resulta ventajoso que la unidad informática central permita para una señal de autorización transmitida derechos de lectura y escritura para el perfil de zona a la unidad informática que transmite el código de autorización.

Esto tiene la ventaja de que una unidad informática de edificio efectúa como instancia adicional de comprobación del código de autorización transmitido. La comunicación de la unidad informática central a la unidad informática de edificio del código de autorización transmitido y la transmisión de la señal de autorización de vuelta a la unidad informática central se realizan mediante un enlace de comunicación, lo que hace que el funcionamiento del sistema de control de acceso sea seguro.

Resulta ventajoso que, si la comprobación del código de autorización transmitido tiene éxito, la unidad informática central permita derechos de lectura y escritura para el perfil de zona a la unidad informática que transmite el código de autorización.

Esto tiene la ventaja de que, si la comprobación del código de autorización transmitido tiene éxito, la unidad informática central remota permite derechos de lectura y escritura para el perfil de zona a la unidad informática que transmite el código de autorización, lo que hace que el funcionamiento del sistema de control de acceso sea seguro.

Resulta ventajoso que el sistema de control de acceso para la realización del procedimiento comprenda la unidad informática. Resulta ventajoso que el sistema de control de acceso comprenda la unidad informática central. Resulta ventajoso que el sistema de control de acceso comprenda una unidad informática de edificio. Resulta ventajoso que el sistema de control de acceso comprenda un enlace de comunicación asistido por red entre la unidad informática y la unidad informática central. Resulta ventajoso que el sistema de control de acceso comprenda un enlace de comunicación asistido por red entre la unidad informática central y el herraje de puerta. Resulta ventajoso que el sistema de control de acceso comprenda una lectura del código de identificación del soporte de datos portátil mediante una transmisión de datos por parte del lector. Resulta ventajoso que el sistema de control de acceso comprenda un enlace de comunicación asistido por red entre la unidad informática central y una unidad informática de edificio.

Esto tiene la ventaja de que se realizan un enlace de comunicación sencillo y seguro entre la unidad informática y la unidad informática central, un enlace de comunicación sencillo y seguro entre la unidad informática central y el herraje de puerta, una transmisión de datos sencilla y segura del soporte de datos portátil al herraje de puerta y un enlace de comunicación sencillo y seguro entre la unidad informática central y la unidad informática de edificio.

Resulta ventajoso que el herraje de puerta esté dispuesto en una hoja de puerta de una puerta en la zona protegida por el herraje de puerta. Resulta ventajoso que el lector esté dispuesto en un marco de puerta del herraje de puerta. Resulta ventajoso que un procesador esté dispuesto en un marco de puerta del herraje de puerta. Resulta ventajoso que una memoria de datos legible por ordenador esté dispuesta en un marco de

puerta del herraje de puerta. Resulta ventajoso que una unidad emisora y receptora para un enlace de comunicación asistido por red está dispuesta entre la unidad informática central y el herraje de puerta, en un marco de puerta del herraje de puerta. Resulta ventajoso que una alimentación de energía eléctrica esté dispuesta en un marco de puerta del herraje de puerta.

Esto tiene la ventaja de que el herraje de puerta y sus componentes están dispuestos de una manera compacta y protegida contra el vandalismo. Resulta ventajoso que la unidad informática esté dispuesta en la zona protegida por el herraje de puerta.

Esto tiene la ventaja de que desde una zona protegida del edificio puede registrarse en y/o eliminarse del perfil de zona para una zona protegida del edificio un código de identificación de un soporte de datos portátil, lo que hace que el funcionamiento del sistema de control de acceso sea sencillo, flexible y seguro.

Resulta ventajoso que un producto de programa informático comprenda como mínimo un recurso de programa informático que sea adecuado para realizar el procedimiento para hacer funcionar un sistema de control de acceso mediante la realización de como mínimo un paso de procedimiento cuando el recurso de programa informático se carga en como mínimo un procesador del herraje de puerta y/o en como mínimo un procesador de la unidad informática y/o en como mínimo un procesador de la unidad informática central y/o en como mínimo un procesador de la unidad informática de edificio. Resulta ventajoso que una memoria de datos legible por ordenador comprenda un producto de programa informático de este tipo.

A continuación se explican detalladamente algunos ejemplos de realización de la invención por medio de las figuras.

Fig. 1: representación esquemática del procedimiento de funcionamiento de un sistema de control de acceso;
Fig. 2: vista esquemática de una parte de un herraje de puerta de un sistema de control de acceso según la Fig. 1;
Fig. 3: diagrama de flujo con pasos de un primer ejemplo de realización del procedimiento según la Fig. 1;
Fig. 4: diagrama de flujo con pasos de un segundo ejemplo de realización del procedimiento según la Fig. 1;
Fig. 5: diagrama de flujo con pasos de un tercer ejemplo de realización del procedimiento según la Fig. 1;
Fig. 6: diagrama de flujo con pasos de un cuarto ejemplo de realización del procedimiento según la Fig. 1;
Fig. 7: diagrama de flujo con pasos de un quinto ejemplo de realización del procedimiento según la Fig. 1; y
Fig. 8: diagrama de flujo con pasos de un sexto ejemplo de realización del procedimiento según la Fig. 1.

La Fig. 1 muestra una representación esquemática del procedimiento de funcionamiento de un sistema de control de acceso en un edificio. En el sentido de la presente invención, el término edificio debe interpretarse ampliamente. Un edificio incluye al menos una zona protegida. La puerta 5 permite el acceso a esta zona protegida del edificio. La zona protegida puede ser un cuarto, un corredor, un hueco de escalera, un ascensor, un ala, una sala, un garaje, un patio de luces, un jardín, una vivienda, una oficina, una consulta, una habitación de hotel, un laboratorio, una celda, etc. del edificio.

La puerta 5 tiene, según la Figura 1, como mínimo una hoja de puerta 51, como mínimo un herraje de puerta 1, como mínimo un cerco de puerta 52 y como mínimo un umbral de puerta 53. El cerco de puerta 52 está anclado de manera fija y estable en la mampostería del edificio. La puerta 5 puede abrirse y cerrarse. El acceso a la zona protegida del edificio se realiza cruzando el umbral 53 con la puerta 5 abierta. Con la puerta 5 cerrada no hay acceso a la zona protegida del edificio.

El herraje de puerta 1 presenta, según la Figura 2, como mínimo una guarnición de puerta 11 con como mínimo un pestillo 16 y como mínimo un picaporte 17. La guarnición de puerta 11 tiene un herraje interior y un herraje exterior. Entre el herraje interior y el herraje exterior, la guarnición de puerta forma una cavidad. El herraje interior está dispuesto en el lado de la puerta 5 que mira hacia el interior del edificio o hacia el interior de la zona protegida del edificio. Tanto en el herraje interior como en el herraje exterior puede estar dispuesto un picaporte 17. El herraje exterior está dispuesto en el lado de la puerta 5 que mira hacia el exterior del edificio o hacia el exterior de la zona protegida del edificio. La guarnición de puerta 11 está fabricada como mínimo por secciones de alta resistencia y en acero inoxidable templado, acero para resortes, etc. para lograr una protección contra el sabotaje. Estando la puerta 5 cerrada, el pestillo 16 está bloqueado en como mínimo un cerradero 54 del cerco de puerta 52. Estando la puerta 5 abierta, el pestillo 16 no está bloqueado en el

cerradero 54 del cerco de puerta 52. El pestillo 16 puede accionarse ejerciendo presión sobre el picaporte 17. El pestillo 16 y el picaporte 17 están acoplados entre sí en arrastre de fuerza mediante un acoplamiento 15. El acoplamiento 15 puede activarse o desactivarse mediante el movimiento de como mínimo una palanca de acoplamiento. Estando el acoplamiento 15 activado, un accionamiento del picaporte 17 se transmite al pestillo 16. Estando el acoplamiento 15 desactivado, un accionamiento del picaporte 17 no se transmite al pestillo 16. En este caso, el picaporte 17 y el pestillo 16 están desacoplados y la puerta 5 cerrada no puede abrirse accionando el picaporte 17. Como mínimo un actuador 18 puede mover la palanca de acoplamiento y activar o desactivar el acoplamiento 15. El actuador 18 es, por ejemplo, un motor eléctrico, que recibe energía eléctrica de como mínimo una alimentación de energía eléctrica 19 y mueve la palanca de acoplamiento. El actuador 18 se activa mediante como mínimo una señal de acceso. Si no está presente ninguna señal de acceso el acoplamiento 15 está desactivado y si está presente una señal de acceso el acoplamiento 15 está activado. Resulta ventajoso que la activación del acoplamiento 15 esté limitada en el tiempo a unos pocos segundos, por ejemplo cinco segundos, etc., de manera que el actuador 18 desactive automáticamente el acoplamiento 15 una vez transcurrido este intervalo de tiempo. Sin embargo, tal intervalo de tiempo corto no es forzoso. Conociendo la presente invención, el técnico en la materia puede también hacer que el acoplamiento 15 se active para intervalos de tiempo de cualquier duración. La alimentación de energía eléctrica 19 está dispuesta también en la cavidad de la guarnición de puerta 15 y consta de una batería o un acumulador o una pila de combustible o una célula solar con una autonomía energética de un año, preferentemente dos años. En el herraje de puerta 1 puede estar dispuesta también como mínimo una lámpara, como un *Light Emitting Diode* (LED), un *Organic Light Emitting Diode* (OLED), etc. Por ejemplo está dispuesto un LED multicolor que pueda encenderse en distintos colores, como verde, rojo, amarillo, azul, etc. Por ejemplo están dispuestos varios LED que puedan encenderse en distintos colores, como verde, rojo, amarillo, azul, etc. En el herraje de puerta 1 puede estar dispuesto también como mínimo un altavoz que pueda emitir como mínimo un sonido. El encendido de las lámparas y/o el sonido del altavoz puede(n) ser percibido(s) por una persona que esté en la zona de la puerta y puede(n) reproducir como mínimo una información de estado. Por ejemplo, en caso de estar presente una señal de acceso la lámpara puede activarse con un parpadeo verde; por ejemplo, en caso de estar presente una señal de perturbación la lámpara puede parpadear en color rojo. Por ejemplo, en caso de estar presente una señal de acceso el altavoz puede activarse con un sonido de 500 Hz; por ejemplo, en caso de estar presente una señal de perturbación el altavoz puede activarse con un sonido de 1.000 Hz.

En la guarnición de puerta 11 está dispuesto como mínimo un lector 10, que recibe energía eléctrica de la alimentación de energía eléctrica 19. El lector 10 presenta como mínimo una antena de radiofrecuencia, un lector de ranura magnético, un lector de ranura electrónico, un sensor biométrico, etc. para una transmisión de datos 21 de como mínimo un soporte de datos portátil 2. A continuación se explican algunos ejemplos de realización del soporte de datos portátil 2:

- La transmisión de datos 21 se basa por ejemplo en una transmisión de datos 21 sin contacto, como *Radio Frequency Identification Device* (**RFID** según ISO11785). Las radiofrecuencias están por ejemplo en bandas de 125 kHz, 13,6 MHz, etc. El soporte de datos portátil 2 es un RFID con como mínimo una bobina eléctrica y como mínimo una memoria de datos legible por ordenador, en la que está almacenado como mínimo un código de identificación. El RFID no tiene alimentación eléctrica propia. El RFID tiene forma, por ejemplo, de tarjeta de crédito o está integrado en un llavero. La antena del lector 10 emite radiofrecuencias. El alcance de la antena es de unos pocos centímetros. Cuando el RFID entra en el alcance del enlace de radiofrecuencia 21, el RFID es activado energéticamente por la radiofrecuencia mediante la bobina eléctrica, y el código de identificación del RFID almacenado en la memoria de datos legible por ordenador se envía mediante la bobina eléctrica del RFID a la antena del lector 10.
- La transmisión de datos 21 se basa por ejemplo en una transmisión de datos 21 sin contacto, como Bluetooth (IEEE802.15.1), ZigBee (IEEE802.15.4), WiFi (IEEE802.11), etc. Las radiofrecuencias están por ejemplo en bandas de 800 a 900 MHz, 1.800 a 1.900 MHz, 1,7 a 2,7 GHz, etc. El alcance de la antena varía entre unos pocos metros en el caso de Bluetooth y ZigBee y unos pocos cientos de metros en el caso de WiFi. El soporte de datos portátil 2 es un equipo portátil, como un teléfono móvil, un *Personal Digital Assistant* (PDA), etc., con como mínimo una antena, como mínimo un procesador, como mínimo una memoria de datos legible por ordenador y una alimentación eléctrica propia. La antena del lector 10 emite radiofrecuencias con señales de consulta. Cuando el equipo portátil entra en el alcance del enlace de radiofrecuencia 21 y recibe una señal de consulta del lector 10, la antena del equipo portátil envía una señal de respuesta a la antena del lector 10. El código de identificación almacenado en la memoria de datos legible por ordenador del equipo portátil se envía mediante la antena del equipo portátil a la antena del lector 10.
- Sin embargo, la transmisión de datos 21 puede basarse también en una lectura con contacto de una banda magnética y/o de una memoria de datos electrónica. En este caso, el soporte de datos portátil 2 es una tarjeta con una banda magnética y/o con una memoria de datos electrónica. La banda

magnética y/o la memoria de datos electrónica la(s) lee un lector de ranura magnético o un lector de ranura electrónico del lector 10.

- La transmisión de datos 21 también puede basarse en la lectura de una señal biométrica mediante un sensor biométrico. En este caso, el soporte de datos portátil 2 es la yema de un dedo de una persona, una mano de una persona, una cara de una persona, un iris de una persona, un cuerpo de una persona, un olor de una persona, etc., que un sensor biométrico del lector 10 lee como huella dactilar, geometría de la mano, perfil de la cara, perfil del iris, exploración de la retina, termograma, olor, peso, voz, firma, etc.

En la guarnición de puerta 11 están dispuestos como mínimo una unidad emisora y receptora 12, como mínimo un procesador 13 y como mínimo una memoria de datos legible por ordenador 14, que reciben energía eléctrica de la alimentación de energía eléctrica 17. La unidad emisora y receptora 12 realiza como mínimo un enlace de comunicación asistido por red 41 entre el herraje de puerta 1 y como mínimo una unidad informática central 4. La unidad emisora y receptora 12, el procesador 13 y la memoria de datos legible por ordenador 14 están dispuestos en como mínimo una placa de circuitos impresos y conectados entre sí mediante como mínimo una línea de señales. Desde la memoria de datos legible por ordenador 14 se carga y se ejecuta en el procesador 13 como mínimo un recurso de programa informático. El recurso de programa informático controla la comunicación entre la unidad emisora y receptora 12, el procesador 13 y la memoria de datos legible por ordenador 14. El recurso de programa informático controla también el enlace de comunicación 41.

Como mínimo una unidad informática central 4 tiene como mínimo una unidad emisora y receptora 42, como mínimo un procesador 43 y como mínimo una memoria de datos legible por ordenador 44. La unidad emisora y receptora 42 realiza como mínimo un enlace de comunicación asistido por red 41 entre la unidad informática central 4 y como mínimo un herraje de puerta 1 y/o como mínimo un enlace de comunicación asistido por red 31, 31' entre la unidad informática central 4 y como mínimo una unidad informática 3. Desde la memoria de datos legible por ordenador 44 se carga y se ejecuta en el procesador 43 como mínimo un recurso de programa informático. El recurso de programa informático controla la comunicación entre la unidad emisora y receptora 42, el procesador 43 y la memoria de datos legible por ordenador 44. El recurso de programa informático controla también el enlace de comunicación 31, 31', 41, 41'. La unidad informática central 4 puede ser un microordenador, como una estación de trabajo, un ordenador personal (PC), etc. La unidad informática central 4 puede ser una interconexión jerárquica de varios microordenadores. La unidad informática central 4 puede estar dispuesta en el edificio y/o alejada del edificio. En una forma de realización, el procesador 43 y una primera memoria de datos legible por ordenador 44 pueden estar dispuestos en una central para el mantenimiento del sistema de control de acceso, mientras que otra memoria de datos legible por ordenador 44 está dispuesta en el edificio del sistema de control de acceso.

Al menos una unidad informática 3 presenta como mínimo una unidad emisora y receptora 32, como mínimo un procesador 33 y como mínimo una memoria de datos legible por ordenador 34. La unidad emisora y receptora 32 realiza como mínimo un enlace de comunicación asistido por red 41, 41' entre la unidad informática 3 y como mínimo una unidad informática central 4. Desde la memoria de datos legible por ordenador 34 se carga y se ejecuta en el procesador 33 como mínimo un recurso de programa informático. El recurso de programa informático controla la comunicación entre la unidad emisora y receptora 32, el procesador 33 y la memoria de datos legible por ordenador 34. La unidad informática 3 puede ser un microordenador portátil, como un PC, un ordenador portátil, un *Netbook*, un teléfono móvil, un PDA, etc. El recurso de programa informático controla también el enlace de comunicación 41. Así, desde la unidad informática 3 es posible, mediante un recurso de programa informático, establecer, mantener y terminar de nuevo un enlace de comunicación asistido por red 41, 41' entre la unidad informática 3 y la unidad informática central 4. El recurso de programa informático puede ser un programa informático para ver páginas asistidas por ordenador de la *World Wide Web*. Se conocen navegadores de este tipo con los nombres Internet Explorer, Firefox, Opera, etc. La unidad informática 3 puede estar dispuesta en el edificio y/o alejada del edificio.

Al menos una unidad informática de edificio 6 presenta como mínimo una unidad emisora y receptora 62, como mínimo un procesador 63 y como mínimo una memoria de datos legible por ordenador 64. La unidad emisora y receptora 62 realiza como mínimo un enlace de comunicación asistido por red 61, 61' entre la unidad informática de edificio 6 y la unidad informática central 4. Desde la memoria de datos legible por ordenador 64 se carga y se ejecuta en el procesador 63 como mínimo un recurso de programa informático. El recurso de programa informático controla la comunicación entre la unidad emisora y receptora 62, el procesador 63 y la memoria de datos legible por ordenador 64. El recurso de programa informático controla también el enlace de comunicación 61, 61'. La unidad informática de edificio 6 puede ser un microordenador, como una estación de trabajo, un ordenador personal (PC), etc. La unidad informática de edificio 6 puede ser

una interconexión jerárquica de varios microordenadores. La unidad informática de edificio 6 puede estar dispuesta en el edificio y/o alejada del edificio.

A continuación se explican algunos ejemplos de realización del enlace de comunicación 31, 31', 41, 41', 61, 61':

- El enlace de comunicación 31, 31', 41, 41', 61, 61' puede ser una red, como Ethernet, ARCNET, etc., con como mínimo una línea de señales eléctrica u óptica. La red permite una comunicación bidireccional según protocolos de red ya conocidos y acreditados, como *Transmision Control Protocol / Internet-Protocol* (TCP/IP), *Hypertext Transfer Protocol* (HTML), *Simple Mail Transfer Protocol* (SMTP), *Internet Message Access Protocol* (IMAP), *Internet Packet Exchange* (IPX), etc. Los usuarios de la red pueden direccionarse de manera inequívoca mediante direcciones de red. Para aumentar la seguridad en el enlace de comunicación 31, 31', 41, 41', 61, 61', la transmisión de los datos relevantes para la seguridad se realiza en forma codificada mediante un enlace de comunicación codificado 31', 41', 61'. Como protocolos de codificación ya conocidos pueden mencionarse *Secure Sockets Layer* (SSL), *Secure Multipurpose Internet Mail Extensions* (S/MIME), etc. El protocolo de codificación está colocado en el modelo de referencia *Open Systems Interconnection* (OSI) encima de la capa de transporte TCP y debajo de programas de aplicación como HTML o SMTP. Con 31, 41, 61 se designa un enlace de comunicación no codificado.
- El enlace de comunicación 31, 41, 61 puede ser una red de radiotelefonía, como *Global Systems for Mobile Communications* (GSM), *General Radio Packet Services* (GPRS), *Enhanced Data Rate for GSM Evolution* (EDGE), *Universal Mobile Telecommunications System* (UMTS), *High Speed Download Packet Access* (HSDPA), etc. Las frecuencias utilizadas por la red de radiotelefonía se hallan, en GSM y GPRS, en bandas de 800 a 900 MHz y de 1.800 a 1.900 MHz y, en UMTS y HSDPA, de 700 a 900 MHz y de 1,7 a 2,7 GHz.
- El enlace de comunicación 31, 41, 61 puede ser una red telefónica fija, como *Public Switched Telecommunication Network* (PSTN). La red telefónica fija puede tener una configuración analógica y/o digital. En el caso de una red telefónica fija analógica se transmiten señales de audio analógicas. El ancho de banda está limitado aquí a la gama de frecuencias de 300 a 3.400 Hz. Además de una señal vocal se transmiten otras señales, como una señal de marcación, una señal de llamada, etc. Una red telefónica fija digital se conoce como *Integrated Services Digital Network* (ISDN), *Asymetric Digital Subscriber Line* (ADSL), *Very High Data Rate Digital Subscriber Line* (VDSL), etc. En el caso del ADSL se utiliza una gama de frecuencias considerablemente mayor, de 200 Hz a 1,1 MHz.

Conociendo la presente invención, el técnico en la materia también puede realizar el enlace de comunicación 31, 41, 61 mediante una red de radiotelefonía y/o una red telefónica fija en forma codificada.

El sistema de control de acceso gestiona el acceso a una zona protegida del edificio mediante como mínimo un perfil de zona. El perfil de zona es, por ejemplo, un archivo legible por ordenador y puede estar almacenado, al menos en parte, en una memoria de datos legible por ordenador 14 del herraje de puerta 1 y/o en una memoria de datos legible por ordenador 44 de la unidad informática central 4. Un perfil de zona se refiere a una zona protegida del edificio y comprende como mínimo una entidad; y para esta entidad el perfil de zona comprende distintos datos como: apellido, nombre de pila, código de identificación, derechos de lectura, derechos de escritura, historial, zona horaria, validez, etc.

- Con "entidad" se designa como mínimo una persona y/o un objeto real, entidad que tiene para este código de identificación acceso a esta zona protegida del edificio. La persona puede ser un humano o un animal. El objeto real puede ser un vehículo, una paleta, un contenedor, un robot, etc.
- Con "apellido" y "nombre de pila" se designan el apellido y el nombre de pila de la entidad. En el caso de una persona, se indican el apellido y el nombre de pila de la persona, tal y como se indican en documentos oficiales, como un documento nacional de identidad, un documento de viaje, etc., de esta persona.
- El código de identificación es, por ejemplo, como mínimo una serie de cifras, que puede estar o no estar codificada, con la que la entidad ha de identificarse para obtener acceso a esta zona protegida del edificio. La serie de cifras puede ser numérica, alfanumérica, etc. El código de identificación puede ser también como mínimo un archivo autónomo, que puede estar o no estar codificado. El código de identificación puede ser también como mínimo una señal biométrica de la entidad, que puede estar o no estar codificada como archivo autónomo.
- Por "derechos de lectura" se entiende una autorización de la entidad para leer el contenido del perfil de zona. Por "derechos de escritura" se entiende una autorización de la entidad para leer y modificar el contenido del perfil de zona.
- Con "historial" se entienden accesos de la entidad a esta zona protegida del edificio almacenados y/o salidas de la entidad de esta zona protegida del edificio almacenadas. El historial comprende, por

ejemplo, la fecha y la hora de cada acceso a esta zona protegida del edificio y la fecha y la hora de cada salida de esta zona protegida del edificio.

- Con "zona horaria" se designa una limitación temporal del acceso de la entidad a esta zona protegida del edificio. La zona horaria puede comprender sólo determinadas horas de una semana, por ejemplo para una entidad que haya de limpiar esta zona protegida del edificio los días laborables entre las 20:00 horas y las 21:00 horas. Sin embargo, la zona horaria también puede ser ilimitada, por ejemplo para una persona que viva de forma permanente en esta zona protegida del edificio. Una zona horaria puede repetirse un número arbitrario de veces, pero también puede durar sólo una vez, por ejemplo si una persona pasa una única noche en una habitación de hotel como zona protegida del edificio. Para esta persona, la zona horaria comienza entonces a las doce del mediodía del primer día y dura toda la noche hasta las once de la mañana del día siguiente.
- Con "validez" se indica si el código de identificación para esta zona protegida del edificio es válido en el momento actual. Si un código de identificación ha sido válido en un momento anterior y no lo es en el momento actual, esta validez anterior puede estar provista de una fecha y una hora de esta modificación.

Durante el funcionamiento del sistema de control de acceso se realiza un mantenimiento de los datos del perfil de zona. A continuación, se explican algunos ejemplos de realización al respecto:

- La zona protegida del edificio es, por ejemplo, varias oficinas de una empresa en las que los días laborables trabajan varias personas. Para las oficinas de esta empresa existen varios perfiles de zona, con un perfil de zona para cada oficina. Si ahora una de estas personas cambia de actividad y ya no trabaja en la antigua oficina, sino en una nueva oficina de la empresa, deben modificarse los perfiles de zona para esta antigua oficina y para esta nueva oficina. Bien se eliminan en el perfil de zona para la antigua oficina los datos relativos a la entidad, al apellido, al nombre de pila de esta persona, o bien se anula la validez para esta persona en el perfil de zona para la antigua oficina, o bien se pone a cero el dato "zona horaria" en el perfil de zona para la antigua oficina, es decir que no se da acceso a ninguna hora. En el perfil de zona para la nueva oficina se registran los datos relativos a la entidad, al apellido, al nombre de pila, al código de identificación y a la zona horaria para esta persona. La persona no tiene ni derechos de lectura ni derechos de escritura en el perfil de zona para la nueva oficina.
- La zona protegida del edificio es, por ejemplo, una vivienda donde vive de forma permanente una familia de varias personas. El perfil de zona para esta vivienda comprende sólo datos relativos a las personas de la familia. Si ahora la familia se va de vacaciones y abandona la vivienda durante dos semanas y el vecino ha de regar las plantas de la vivienda durante estas dos semanas, debe modificarse el perfil de zona para esta vivienda. En el perfil de zona para esta vivienda se registra una nueva entidad para el vecino, con datos relativos al apellido, al nombre de pila, al código de identificación y a la zona horaria. El vecino no tiene ni derechos de lectura ni derechos de escritura. La zona horaria es de dos semanas, tanto como duran las vacaciones.

Para realizar el mantenimiento de un perfil de zona se transmite desde la unidad informática 3 como mínimo un código de autorización a la unidad informática central 4. El código de autorización es, de manera similar al código de identificación, como mínimo una serie de cifras, que puede estar o no estar codificada. La serie de cifras puede ser numérica, alfanumérica, etc. El código de autorización también puede ser como mínimo un archivo autónomo, que puede estar o no estar codificado. El código de autorización puede ser también como mínimo una señal biométrica de la entidad, que puede estar o no estar codificada como archivo autónomo. El código de autorización puede ser idéntico al código de identificación. El código de autorización puede ser una dirección, por ejemplo una dirección de correo (dirección de e-mail) para una comunicación según SMTP, IMAP, etc.

Se comprueba si el código de autorización transmitido coincide con un código de autorización válido para un perfil de zona. Cada perfil de zona está vinculado a un código de autorización válido. El código de autorización válido puede estar almacenado en la unidad informática central 4 o en la unidad informática de edificio 6. La comprobación puede realizarse por la unidad informática central 4 y/o la unidad informática de edificio 6. En una configuración ventajosa del procedimiento, el código de autorización transmitido lo transmite la unidad informática central 4 mediante un enlace de comunicación 61, 61' a la unidad informática de edificio 6, que comprueba el código de autorización transmitido y, si la comprobación tiene éxito, transmite una señal de autorización mediante un enlace de comunicación 61, 61' a la unidad informática central 4.

Si la comprobación del código de autorización transmitido tiene éxito, la unidad informática central 4 permite a la unidad informática 3 que transmita el código de autorización derechos de lectura y escritura para el perfil de zona que está vinculado al código de autorización transmitido. Si la comprobación del código de autorización transmitido la ha realizado la unidad informática de edificio 6, la unidad informática central 4 no permite derechos de lectura y escritura para un perfil de zona hasta haberse transmitido una señal de

autorización correspondiente. Para un perfil de zona permitido, la unidad informática central 4 transmite a la unidad informática 3 una señal de permisión mediante el enlace de comunicación 31, 31'. Desde la unidad informática 3 se modifica mediante el enlace de comunicación 31, 31' el perfil de zona permitido. Para ello, la unidad informática 3 transmite como mínimo una señal de modificación a la unidad informática central 4 mediante el enlace de comunicación 31, 31', la unidad informática central 4 efectúa una modificación del perfil de zona para una señal de modificación recibida. La modificación del perfil de zona puede comprender un borrado, una adición, un cambio de un dato del perfil de zona, como el apellido, el nombre de pila, el código de identificación, los derechos de lectura, los derechos de escritura, el historial, la zona horaria, la validez, etc.

Las Figuras 3 a 8 muestran diagramas de flujo de pasos de ejemplos de realización del procedimiento para hacer funcionar un sistema de control de acceso. A continuación se describen los distintos pasos:

- Según la Figura 3, en un paso S1 se almacena un perfil de zona T1 con un código de identificación válido T2' en la unidad informática central 4 y queda disponible en la misma.
- Según las Figuras 4 y 5, en un paso S1 la unidad informática central 4 transmite mediante un enlace de comunicación 41, 41' un perfil de zona T1 con un código de identificación válido T2' a una dirección de red del herraje de puerta 1 que da acceso a la zona protegida a la que se refiere el perfil de zona T1. El paso S1 puede realizarse según sea necesario, por ejemplo a intervalos de tiempo regulares, como semanalmente, mensualmente, etc., y/o después de realizarse una modificación del perfil de zona T1 de la zona protegida por el herraje de puerta 1. El enlace de comunicación 41, 41' puede mantenerse permanentemente o puede establecerse sólo para los intereses de la transmisión del perfil de zona T1.
- Según las Figuras 3 a 5, en un paso S2 un lector 10 del herraje de puerta 1 lee un código de identificación T2 de un soporte de datos portátil 2 por transmisión de datos 21.
- Según la Figura 3, en un paso S3 el herraje de puerta 1 transmite mediante un enlace de comunicación 41, 41' un código de identificación T2 leído a la dirección de red de la unidad informática central 4.
- Según la Figura 3, la unidad informática central 4 recibe mediante el enlace de comunicación 41, 41' el código de identificación T2 leído. Según las Figuras 4 y 5, el código de identificación T2 leído está disponible en el herraje de puerta 1. Según la Figura 3, en un paso S4 la unidad informática central 4 comprueba si el código de identificación T2 leído coincide con un código de identificación válido T2' para la zona protegida por el herraje de puerta 1, código de identificación válido que está almacenado en el perfil de zona T1. Si el código de identificación T2 leído coincide con el código de identificación válido T2', la unidad informática central 4 genera una señal de acceso T4 y, mediante un enlace de comunicación 41, 41', transmite ésta a la dirección de red del herraje de puerta 1 que ha leído el código de identificación T2 y lo ha transmitido a la unidad informática central 4. Si el código de identificación T2 leído no coincide con el código de identificación válido T2', la unidad informática central 4 genera una señal de bloqueo T4' y, mediante un enlace de comunicación 41, 41', transmite ésta a la dirección de red del herraje de puerta 1 que ha leído el código de identificación T2 y lo ha transmitido a la unidad informática central 4.
- Según las Figuras 4 y 5, en un paso S4 el herraje de puerta 1 comprueba si el código de identificación T2 leído coincide con un código de identificación válido T2' para la zona protegida por el herraje de puerta 1, código de identificación válido T2' que está almacenado en el perfil de zona T1. Si el código de identificación T2 leído coincide con el código de identificación válido T2', el herraje de puerta 1 genera una señal de acceso T4. Si el código de identificación T2 leído no coincide con el código de identificación válido T2', el herraje de puerta 1 genera una señal de bloqueo T4'. Según la Figura 5, el herraje de puerta 1 transmite a la dirección de red de la unidad informática central 4, mediante un enlace de comunicación 41, 41', un código de identificación T2 leído y la señal de bloqueo T4' generada para este código de identificación T2 leído.
- Según la Figura 5, la unidad informática central 4 recibe mediante el enlace de comunicación 41, 41' un código de identificación T2 leído y una señal de bloqueo T4' generada para este código de identificación T2. Según la Figura 5, en un paso S4' la unidad informática central 4 comprueba si el código de identificación T2 leído coincide con un código de identificación válido T2' para la zona protegida por el herraje de puerta 1, código de identificación válido T2' que está almacenado en el perfil de zona T1. Si el código de identificación T2 leído coincide con el código de identificación válido T2', la unidad informática central 4 genera una señal de acceso T4''. Según la Figura 5, la unidad informática central 4 transmite un código de identificación T2 leído y la señal de acceso T4'' generada para este código de identificación T2 leído, mediante un enlace de comunicación 41, 41', a la dirección de red del herraje de puerta 1 que ha leído el código de identificación T2 y lo ha transmitido a la unidad informática central 4. Si el código de identificación T2 leído no coincide con el código de identificación válido T2', la unidad informática central 4 genera una señal de bloqueo T4'''. Según la Figura 5, la unidad informática central 4 transmite un código de identificación T2 leído y la señal de bloqueo T4''' generada para este código de identificación T2 leído, mediante un enlace de comunicación 41, 41', a la dirección de red del herraje de puerta 1 que ha leído el código de identificación T2 y lo ha transmitido a la unidad informática central 4.
- Según la Figura 3, el herraje de puerta 1 recibe una señal de acceso T4 mediante el enlace de comunicación 41, 41'. Según la Figura 4, en el herraje de puerta 1 se halla una señal de acceso T4.

Según la Figura 5, el herraje de puerta 1 recibe, mediante el enlace de comunicación 41, 41', un código de identificación T2 leído y una señal de acceso T4" generada para este código de identificación T2 leído. Según las Figuras 3 a 5, en un paso S5, para una señal de acceso T4 presente, el herraje de puerta 1 da acceso a la zona protegida por el herraje de puerta 1 y/o se emite una información de acceso, por ejemplo en forma de una lámpara activada y/o de un altavoz activado del herraje de puerta 1.

- Según la Figura 3, el herraje de puerta 1 recibe una señal de bloqueo T4' mediante el enlace de comunicación 41, 41'. Según la Figura 4, en el herraje de puerta 1 está presenta una señal de bloqueo T4'. Según la Figura 5, el herraje de puerta 1 recibe mediante el enlace de comunicación 41, 41' un código de identificación T2 leído y una señal de bloqueo T4"' generada para este código de identificación T2 leído. Según las Figuras 3 a 5, para una señal de bloqueo T4', T4"' presente, en un paso S5' el herraje de puerta 1 no da acceso a la zona protegida por el herraje de puerta 1 y/o se emite una información de bloqueo, por ejemplo en forma de una lámpara activada y/o de un altavoz activado del herraje de puerta 1.
- Según las figuras 6 y 7, en un paso S11 se inicia un mantenimiento de un perfil de zona, para lo que la unidad informática 3 transmite, mediante un enlace de comunicación 31, una petición de mantenimiento de un perfil de zona T1 a la dirección de red de la unidad informática central 4.
- Según las Figuras 6 y 7, la unidad informática central 4 recibe la petición de mantenimiento, el perfil de zona T1 y la dirección de red de la unidad informática 3 mediante el enlace de comunicación 31. Según las Figuras 6 y 7, en un paso S12 la unidad informática central 4 comprueba si el perfil de zona T1 existe en el sistema de control de acceso. Si el perfil de zona T1 existe en el sistema de control de acceso, la unidad informática central 4 transmite una petición de dirección de correo T12 a la dirección de red de la unidad informática 3 mediante el enlace de comunicación 31. Si el perfil de zona T1 no existe en el sistema de control de acceso, la unidad informática central 4 transmite una petición de repetición de petición T12' a la dirección de red de la unidad informática 3 mediante el enlace de comunicación 31.
- Según las Figuras 6 y 7, la unidad informática 3 recibe la petición de dirección de correo T12 mediante el enlace de comunicación 31. Según las Figuras 6 y 7, en un paso S13 la unidad informática 3 transmite una dirección de correo T13 de la unidad informática 3 a la dirección de red de la unidad informática central 4 mediante un enlace de comunicación 31'. La transmisión de la dirección de correo T13 se realiza mediante un enlace de comunicación codificado 31', que la unidad informática 3 constituye mediante una referencia electrónica (hipervínculo) a partir de la petición de dirección de correo T12 recibida.
- Según las Figuras 6 y 7, la unidad informática central 4 recibe la dirección de correo T13 mediante el enlace de comunicación codificado 31'. Según las Figuras 6 y 7, en un paso S14 la unidad informática central 4 transmite una petición de código de autorización T14 a la dirección de red de la unidad informática 3 mediante un enlace de comunicación codificado 31'. Adicionalmente a la petición de código de autorización T14, la unidad informática central 4 puede transmitir a la dirección de red de la unidad informática 3 una petición de confirmación de la dirección de correo T13 de la unidad informática 3.
- Según las Figuras 6 y 7, la unidad informática 3 recibe la petición de código de autorización T14 y, en caso dado, la petición de confirmación de la dirección de correo T13 mediante el enlace de comunicación 31'. Según las Figuras 6 y 7, en un paso S15 la unidad informática 3 transmite un código de autorización T15 y, en caso dado, una confirmación de la dirección de correo T3 a la dirección de red de la unidad informática central 4 mediante un enlace de comunicación codificado 31'.
- Según las Figuras 6 y 7, la unidad informática central 4 recibe el código de autorización T15 y, en caso dado, la confirmación de la dirección de correo T13 mediante el enlace de comunicación codificado 31'. Según la Figura 6, en un paso S16 la unidad informática central 4 transmite una petición de comprobación de código de autorización T16 con el código de autorización T15 y el perfil de zona T1 a una dirección de correo de la unidad informática de edificio 6 mediante un enlace de comunicación 61.
- Según la Figura 6, la unidad informática de edificio 6 recibe la petición de comprobación de código de autorización T16, el código de autorización T15 y el perfil de zona T1 mediante el enlace de comunicación 61. Según la Figura 6, en un paso S17 la unidad informática de edificio 6 comprueba si el código de autorización T15 es válido para el perfil de zona T1. Si el código de autorización T15 es válido para el perfil de zona T1, según la Figura 6 la unidad informática de edificio 6 genera una señal de autorización T17 y transmite ésta a la dirección de red de la unidad informática central 4 mediante un enlace de comunicación codificado 61'. Si el código de autorización T15 no es válido para el perfil de zona T1, según la Figura 6 la unidad informática de edificio 6 genera una señal de no-autorización T17' y transmite ésta a la dirección de red de la unidad informática central 4 mediante el enlace de comunicación codificado 61'. La transmisión de la señal de autorización T17 o de la señal de no-autorización T17' se realiza mediante un enlace de comunicación codificado 61', que la unidad informática de edificio 6 constituye mediante una referencia electrónica (hipervínculo) a partir de la petición de comprobación de código de autorización T16 recibida.
- Según la Figura 7, la petición de comprobación de código de autorización T16, el código de autorización T15 y el perfil de zona T1 están presentes en la unidad informática central 4. Según la Figura 7, en un paso S17 la unidad informática central 4 comprueba si el código de autorización T15 es válido para el perfil de zona T1. Si el código de autorización T15 es válido para el perfil de zona T1, según la Figura 7 la unidad informática central 4 genera una señal de autorización T17. Si el código de autorización T15 no es

válido para el perfil de zona T1, según la Figura 7 la unidad informática central 4 genera una señal de no-autorización T17'.

- Según la Figura 6, la unidad informática central 4 recibe la señal de autorización T17 o la señal de no-autorización T17' mediante el enlace de comunicación codificado 61'. Según la Figura 7, en la unidad informática central 4 está presente una señal de autorización T17 o una señal de no-autorización T17'. Según las Figuras 6 y 7, en un paso S18 la unidad informática central 4 permite, para una señal de autorización T17 presente, derechos de lectura y escritura para el perfil de zona T1. Genera una señal de permisión T18 y transmite la señal de permisión T18 a la dirección de correo de la unidad informática 3 mediante un enlace de comunicación 31.
- Según las Figuras 6 y 7, la unidad informática 3 recibe la señal de permisión T18 mediante el enlace de comunicación 31.
- Según las Figuras 6 a 8, en un paso S19 la unidad informática 3 genera una señal de modificación T19 y transmite ésta a la dirección de red de la unidad informática central 4 mediante un enlace de comunicación 31'. La transmisión de la señal de modificación T19 se realiza mediante un enlace de comunicación codificado 31', que la unidad informática 3 constituye mediante una referencia electrónica (hipervínculo) a partir de la señal de autorización T18 recibida.
- Según las Figuras 6 a 8, la unidad informática central 4 recibe la señal de modificación T19 mediante el enlace de comunicación codificado 31'. Según las Figuras 6 y 7, en un paso S20, para una señal de modificación T19 recibida, la unidad informática central 4 efectúa modificaciones en el perfil de zona T1 y transmite una señal de confirmación de modificación T20 a la dirección de red de la unidad informática 3 mediante un enlace de comunicación codificado 31'.

Conociendo la presente invención, el técnico en la materia puede realizar el enlace de comunicación codificado 31', 61' arriba descrito también mediante un enlace de comunicación no codificado 31, 61.

- Según la Figura 8, en un paso S20 la unidad informática central 4 convierte una señal de modificación T19 en una modificación de un perfil de zona T1 permitido de tal manera que se crea en éste un código de identificación provisional T2*.
- Según la Figura 8, en un paso S21 se compara un código de identificación T2 leído con el código de identificación provisional T2* creado. Si el código de identificación T2 leído se ha leído en el herraje de puerta 1 que da acceso a la zona protegida del perfil de zona T1 permitido con el código de identificación provisional T2* creado, y si el código de identificación T2 leído coincide con este código de identificación provisional T2*, el código de identificación T2 leído se registra como código de identificación válido T2' en el perfil de zona permitido. Si no es éste el caso y el código de identificación T2 leído difiere del código de identificación provisional T2* creado, la unidad informática central 4 genera una señal de error T21.
- Según la Figura 8, en un paso S22 la unidad informática central 4 transmite, para el código de identificación válido T2' registrado en el perfil de zona T1, una señal de confirmación de modificación T20 a la dirección de red de la unidad informática 3 mediante un enlace de comunicación 31, 31'.

Reivindicaciones

1. Procedimiento de funcionamiento de un sistema de control de acceso a una zona protegida de un edificio con como mínimo un herraje de puerta (1) y como mínimo un código de identificación (T2) en un soporte de datos portátil (2); código de identificación (T2) que es leído por un lector (10) del herraje de puerta (1); dándose acceso a la zona protegida por el herraje de puerta (1) si un código de identificación (T2) leído es válido; donde
una unidad informática (3) transmite un código de autorización (T15) a una unidad informática central (4) mediante como mínimo un enlace de comunicación (31, 31');
una unidad informática de edificio (6) comprueba si el código de autorización (T15) transmitido coincide con un código de autorización válido para un perfil de zona (T1);
la unidad informática central (4) permite derechos de lectura y escritura para el perfil de zona (T1) a la unidad informática (3) que transmite el código de autorización (T15) si la comprobación del código de autorización (T15) transmitido tiene éxito;
la unidad informática (3) modifica el perfil de zona (T1) permitido mediante un enlace de comunicación (31, 31');
la unidad informática (3) crea el código de identificación del soporte de datos portátil (2) como código de identificación provisional (T2*) en el perfil de zona (T1) permitido; y
si el lector (10) del herraje de puerta (1) que da acceso a la zona protegida del perfil de zona (T1) permitido lee un código de identificación (T2) que coincide con el código de identificación provisional (T2*), el código de identificación (T2) leído se registra como código de identificación válido (T2') en el perfil de zona (T1) permitido.

2. Procedimiento según la reivindicación 1, caracterizado porque la unidad informática (3) elimina del perfil de zona (T1) permitido, como código de identificación válido (T2'), un código de identificación (T2) de un soporte de datos portátil (2) y/o porque la unidad informática (3) modifica una validez de un código de identificación del perfil de zona (T1) permitido y/o porque la unidad informática (3) registra una entidad en el perfil de zona (T1) permitido y/o porque la unidad informática (3) elimina una entidad del perfil de zona (T1) permitido y/o porque la unidad informática (3) modifica unos derechos de lectura de una entidad del perfil de zona (T1) permitido y/o porque la unidad informática modifica unos derechos de escritura de una entidad del perfil de zona (T1) permitido y/o porque la unidad informática (3) modifica una zona horaria de una entidad del perfil de zona (T1) permitido.

3. Procedimiento según la reivindicación 1, caracterizado porque el código de identificación provisional (T2*) se crea indicando una serie de cifras en el perfil de zona (T1) permitido; y porque, si el lector (10) del herraje de puerta (1) que da acceso a la zona protegida del perfil de zona (T1) permitido lee una serie de cifras que coincide con la serie de cifras del código de identificación provisional (T2*), un código de identificación (T2) leído con la serie de cifras se registra como código de identificación válido (T2') en el perfil de zona (T1) permitido y/o el código de identificación provisional (T2*) se crea indicando un intervalo de tiempo en el perfil de zona (T1) permitido; y, si el lector (10) del herraje de puerta (1) que da acceso a la zona protegida del perfil de zona (T1) permitido lee durante el intervalo de tiempo un código de identificación (T2) que coincide con el código de identificación provisional (T2*), se registra como código de identificación válido (T2') en el perfil de zona (T1) permitido el código de identificación (T2) leído.

4. Procedimiento según una de las reivindicaciones 1 a 3, caracterizado porque un procesador (13) de un herraje de puerta (1) comprueba si un código de identificación (T2) leído por el lector (10) del herraje de puerta (1) coincide con un código de identificación válido (T2') de un perfil de zona (T1) para la zona protegida por el herraje de puerta (1) y/o porque la unidad informática central (4) transmite a un herraje de puerta (1), mediante un enlace de comunicación (41, 41'), como mínimo una parte de un perfil de zona (T1) para la zona protegida por el herraje de puerta (1); y porque un procesador (13) del herraje de puerta (1) comprueba si un código de identificación (T2) leído por el lector (10) del herraje de puerta (1) coincide con un código de identificación válido (T2') del perfil de zona (T1) transmitido y/o porque la unidad informática central (4) transmite a un herraje de puerta (1), mediante un enlace de comunicación (41, 41'), como mínimo una parte de un perfil de zona (T1) para la zona protegida por el herraje de puerta (1); porque un procesador (13) del herraje de puerta (1) comprueba si un código de identificación (T2) leído por el lector (10) del herraje de puerta (1) coincide con un código de identificación válido (T2') del perfil de zona (T1) transmitido; porque, si la comprobación del código de identificación (T2) leído tiene éxito, el procesador (13) transmite una señal de acceso (T4) a un actuador (18) del herraje de puerta; y porque, para la señal de acceso (T4) transmitida, el actuador (18) da acceso a la zona protegida por el herraje de puerta (1).

5. Procedimiento según una de las reivindicaciones 1 a 3, caracterizado porque la unidad informática central (4) comprueba si un código de identificación (T2) leído por un lector (10) de un herraje de

puerta (1) coincide con un código de identificación válido (T2') de un perfil de zona (T1) para la zona protegida por el herraje de puerta (1) del lector (10) y/o porque, mediante un enlace de comunicación (41, 41'), se transmite a la unidad informática central (4) un código de identificación (T2) leído por un lector (10); y porque la unidad informática central (4) comprueba si el código de identificación (T2) leído coincide con un código de identificación válido (T2') de un perfil de zona (T1) para la zona protegida por el herraje de puerta (1) del lector (10) y/o porque, mediante un enlace de comunicación (41, 41'), se transmite a la unidad informática central (4) un código de identificación (T2) leído por un lector (10); y porque la unidad informática central (4) comprueba si el código de identificación (T2) leído coincide con un código de identificación válido (T2') de un perfil de zona (T1) para la zona protegida por el herraje de puerta (1) del lector (10); porque, si la comprobación del código de identificación (T2) leído tiene éxito, la unidad informática central (4) transmite una señal de acceso (T4) a un actuador (18) del herraje de puerta (1) mediante el enlace de comunicación (41, 41'); y porque, para la señal de acceso (T4) transmitida, el actuador (18) da acceso a la zona protegida por el herraje de puerta (1).

6. Procedimiento según una de las reivindicaciones 1 a 5, caracterizado porque la unidad informática central (4) transmite a una unidad informática de edificio (6), mediante un enlace de comunicación (61, 61'), un código de autorización (T15) transmitido; porque la unidad informática de edificio (6) comprueba si el código de autorización (T15) transmitido coincide con un código de autorización válido para un perfil de zona (T1); y porque, si la comprobación del código de autorización (T15) transmitido tiene éxito, la unidad informática de edificio (6) transmite una señal de autorización (T17) a la unidad informática central (4) mediante un enlace de comunicación (61, 61') y/o porque la unidad informática central (4) transmite a una unidad informática de edificio (6), mediante un enlace de comunicación (61, 61'), un código de autorización (T15) transmitido; porque la unidad informática de edificio (6) comprueba si el código de autorización (T15) transmitido coincide con un código de autorización válido para un perfil de zona (T1); porque, si la comprobación del código de autorización (T15) transmitido tiene éxito, la unidad informática de edificio (6) transmite una señal de autorización (T17) a la unidad informática central (4) mediante un enlace de comunicación (61, 61'); y porque, para una señal de autorización (T17) transmitida, la unidad informática central (4) permite derechos de lectura y escritura para el perfil de zona (T1) a la unidad informática (3) que transmite el código de autorización (T15).

7. Procedimiento según una de las reivindicaciones 1 a 6, caracterizado porque, si la comprobación del código de autorización (T15) transmitido tiene éxito, la unidad informática central (4) permite derechos de lectura y escritura para el perfil de zona (T1) a la unidad informática (3) que transmite el código de autorización (T15).

8. Sistema de control de acceso para la realización del procedimiento según una de las reivindicaciones 1 a 7, comprendiendo el sistema de control de acceso una unidad informática (3), una unidad informática central (4), una unidad informática de edificio (6), un soporte de datos portátil (2), que almacena un código de identificación (T2), y un herraje de puerta (1) con un lector (10), comprendiendo el sistema de control de acceso un enlace de comunicación asistido por red (31, 31') entre la unidad informática (3) y la unidad informática central (4) para la transmisión de un código de autorización (T15) a la unidad informática central (4), un enlace de comunicación asistido por red (61, 61') entre la unidad informática central (4) y la unidad informática de edificio (6) y un enlace de comunicación asistido por red (41, 41') entre la unidad informática central (4) y el herraje de puerta (1), sistema de control de acceso en el que el lector (10) lee el código de identificación (T2) del soporte de datos portátil (2) mediante una transmisión de datos (21), donde, si la comprobación del código de autorización (T15) transmitido tiene éxito, la unidad informática central (4) permite derechos de lectura y escritura para el perfil de zona (T1) a la unidad informática (3) que transmite el código de autorización (T15); donde la unidad informática (3) modifica, mediante el enlace de comunicación (31, 31') entre la unidad informática (3) y la unidad informática central (4), el perfil de zona (T1) permitido; donde la unidad informática (3) crea el código de identificación del soporte de datos portátil (2) como código de identificación provisional (T2*) en un perfil de zona (T1) permitido, donde, si el lector (10) lee un código de identificación (T2) que coincide con el código de identificación provisional (T2*), la unidad informática (3) registra el código de identificación (T2) como código de identificación válido (T2') en el perfil de zona (T1) permitido.

9. Sistema de control de acceso según la reivindicación 8, caracterizado porque el perfil de zona (T1) está almacenado, al menos en parte, en una memoria de datos legible por ordenador (43) de la unidad informática central (4) y/o porque el perfil de zona (T1) está almacenado, al menos en parte, en una memoria de datos legible por ordenador (14) del herraje de puerta (1).

10. Sistema de control de acceso según una de las reivindicaciones 8 o 9, caracterizado porque el herraje de puerta (1) está dispuesto en una hoja de una puerta a la zona protegida por el herraje de puerta (1).

11. Sistema de control de acceso según una de las reivindicaciones 8 a 10, caracterizado porque el lector (10) está dispuesto en una guarnición de puerta (11) del herraje de puerta (1) y/o porque un procesador (13) está dispuesto en una guarnición de puerta (11) del herraje de puerta (1) y/o porque una memoria de datos legible por ordenador (14) está dispuesta en una guarnición de puerta (11) del herraje de puerta (1) y/o una unidad emisora y receptora (12) para un enlace de comunicación asistido por red (41) entre la unidad informática central (4) y el herraje de puerta (1) está dispuesta en una guarnición de puerta (11) del herraje de puerta (1) y/o una alimentación de energía eléctrica (19) está dispuesta en una guarnición de puerta (11) del herraje de puerta (1).

12. Sistema de control de acceso según una de las reivindicaciones 8 a 11, caracterizado porque la unidad informática (3) está dispuesta en la zona protegida por el herraje de puerta (1).

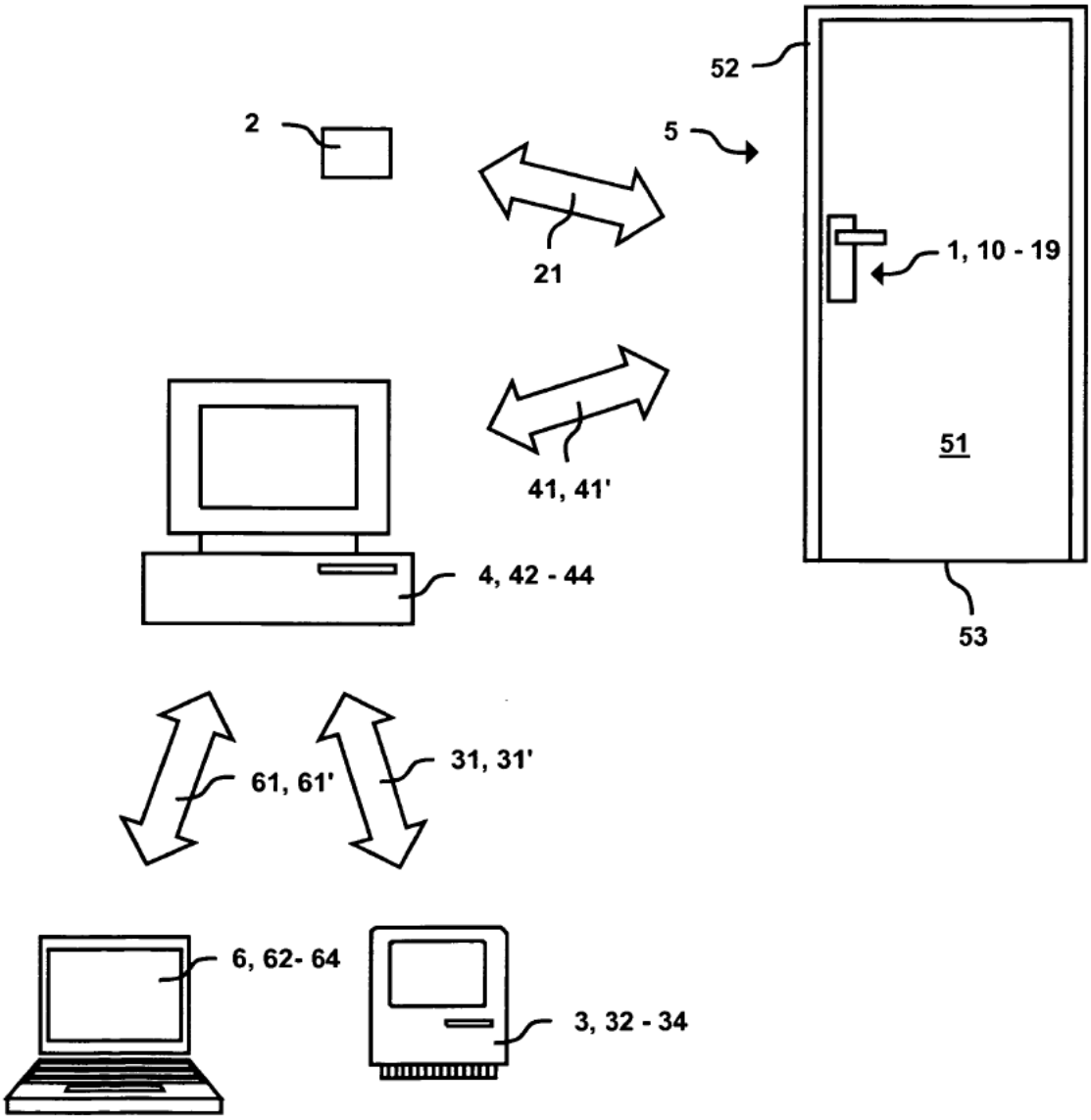

Fig. 1

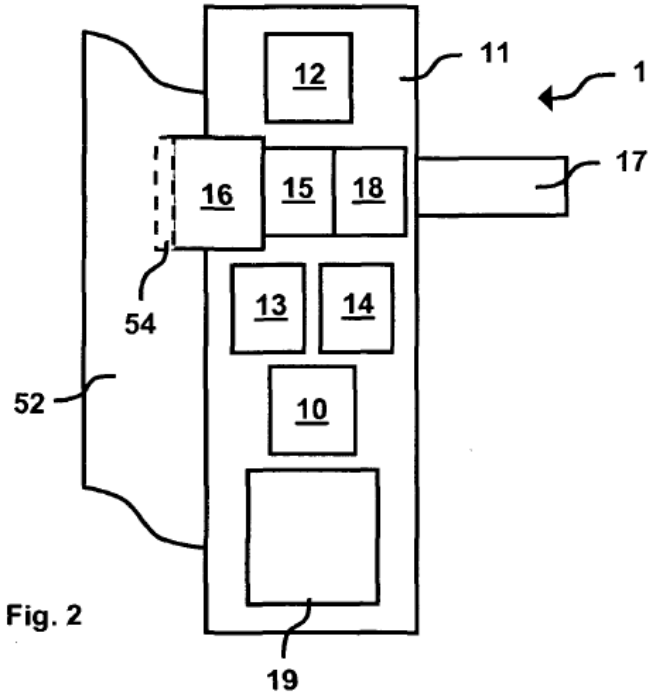
12
11
1
16
15
18
17
54
13
14
52
10
19

Fig. 2

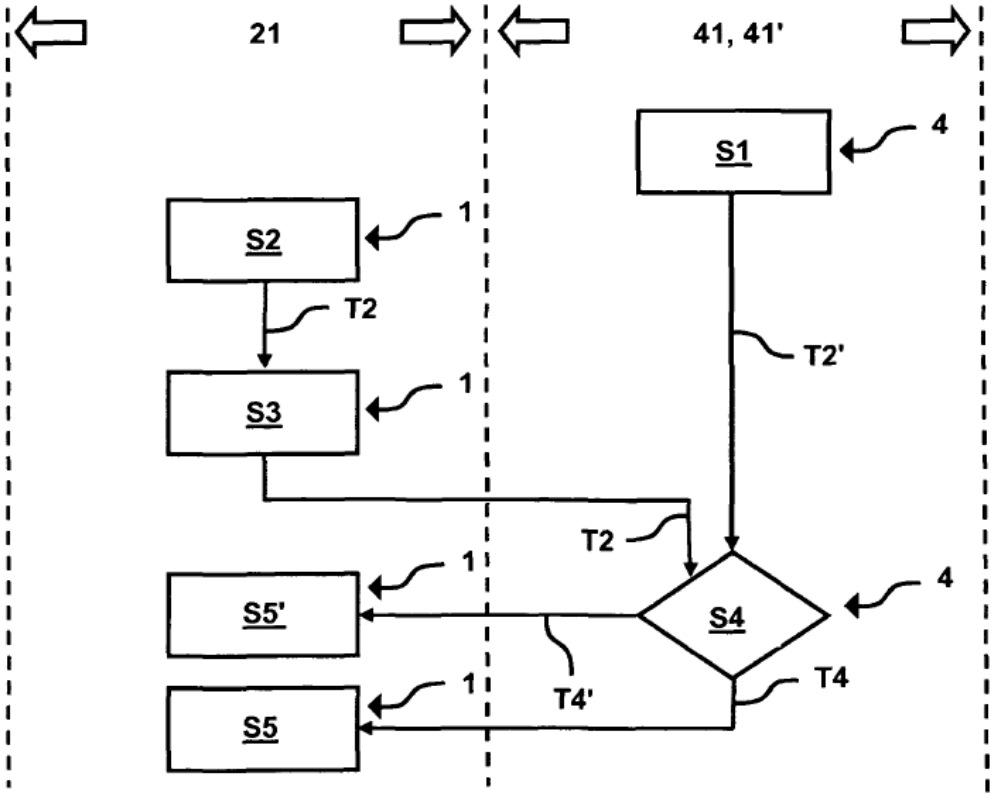
21
41, 41'
S1
4
S2
1
T2
T2'
S3
1
T2
S5'
1
S4
4
T4'
T4
S5
1

Fig. 3

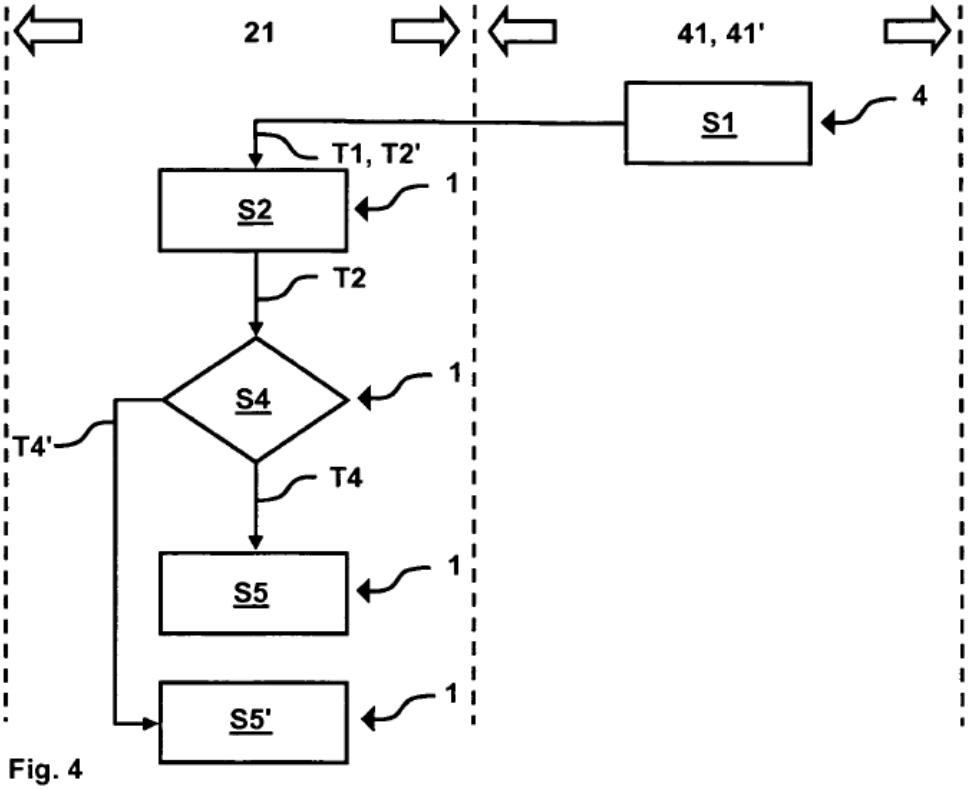
21
41, 41'
S1
4
T1, T2'
S2
1
T2
S4
1
T4'
T4
S5
1
S5'
1

Fig. 4

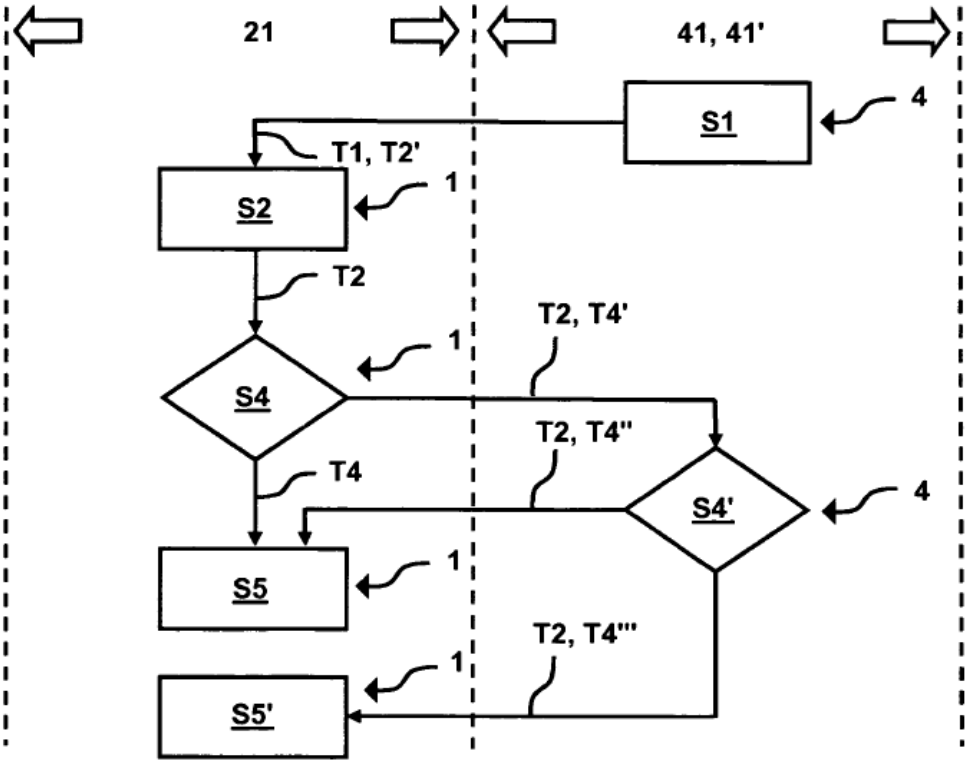
21
41, 41'
S1
4
T1, T2'
S2
1
T2
T2, T4'
S4
1
T2, T4''
T4
S4'
4
S5
1
T2, T4'''
S5'
1

Fig. 5

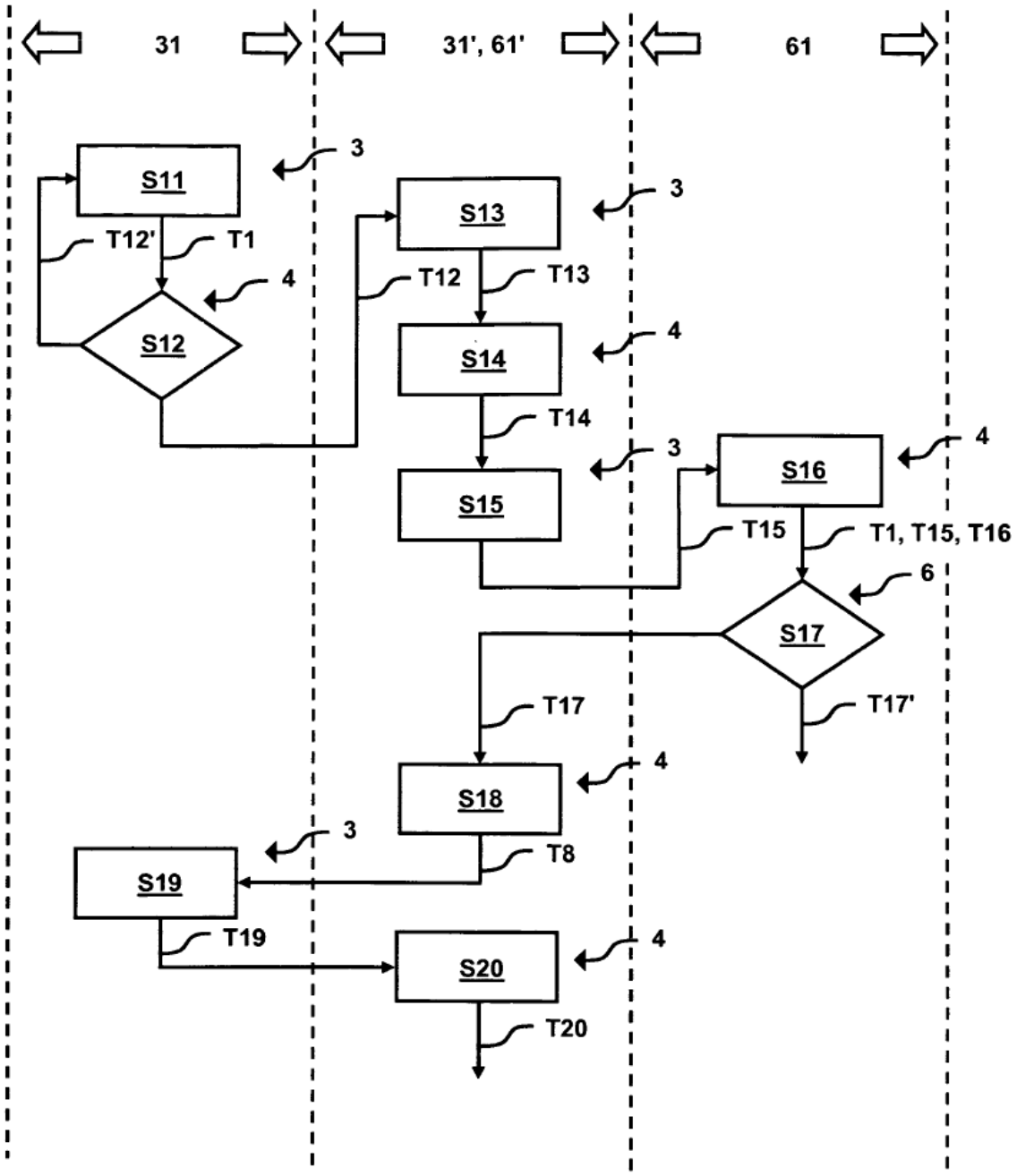
31
31', 61'
61
S11
S12
S13
S14
S15
S16
S17
S18
S19
S20
T12'
T1
T12
T13
T14
T15
T1, T15, T16
T17
T17'
T8
T19
T20
3
4
6

Fig. 6

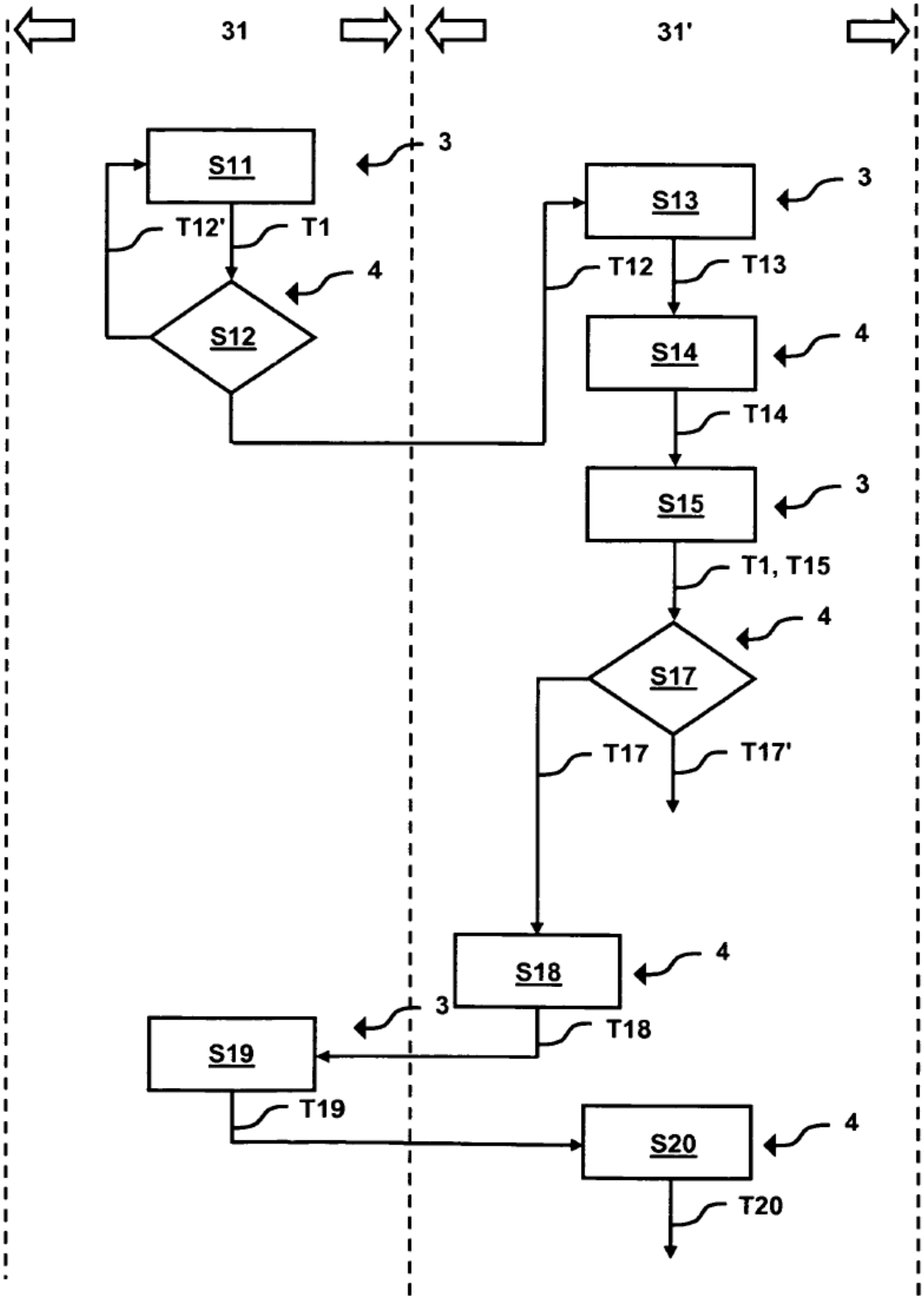
31
31'
S11
3
T12'
T1
4
S12
S13
3
T12
T13
S14
4
T14
S15
3
T1, T15
4
S17
T17
T17'
S18
4
3
T18
S19
T19
S20
4
T20

Fig. 7

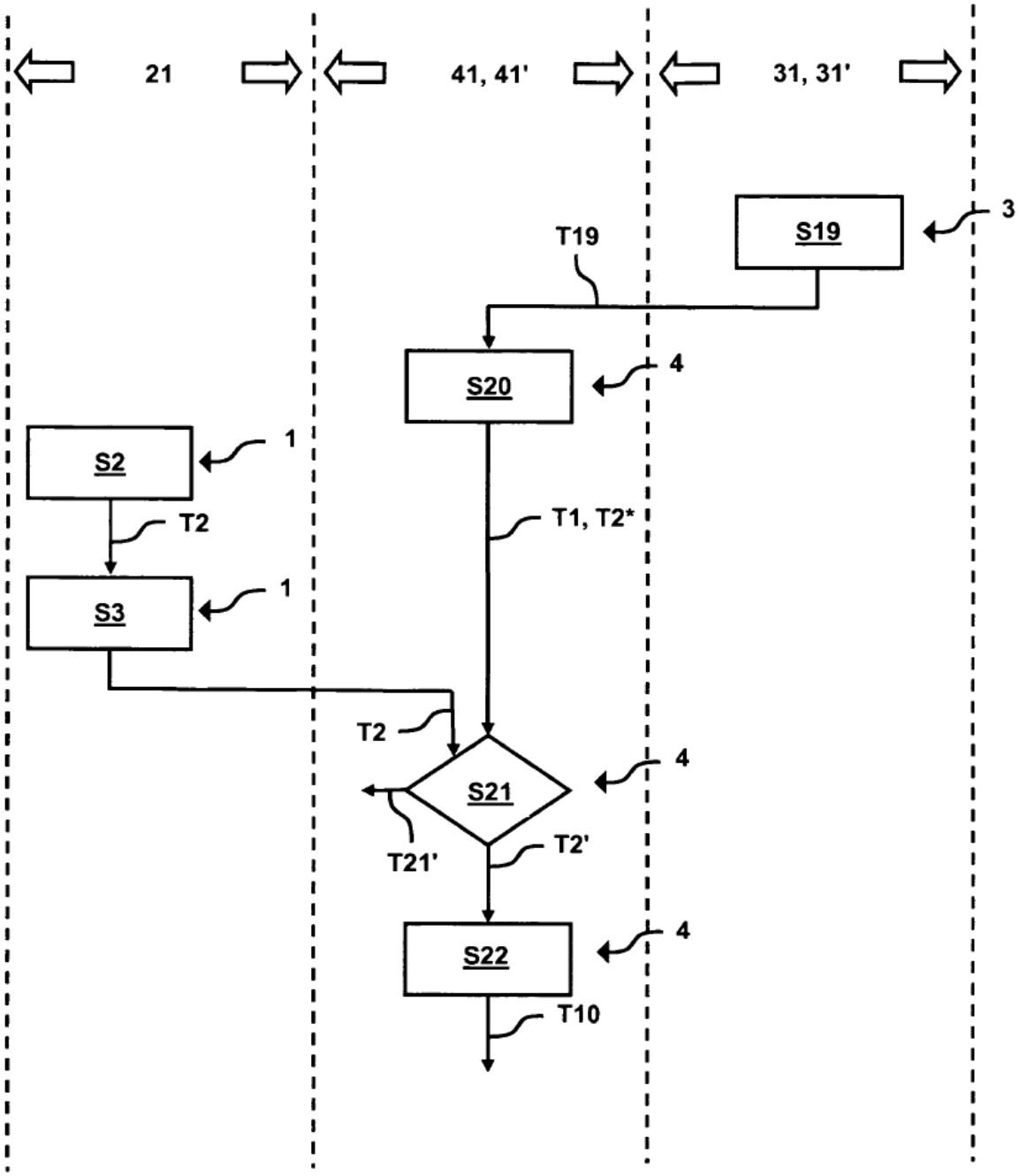
21
41, 41'
31, 31'
S19
3
T19
S20
4
S2
1
T2
T1, T2*
S3
1
T2
S21
4
T21'
T2'
S22
4
T10

Fig. 8